Making an hardware CTF on a single board for my students

About me

- Over caffeinated wolf
- Voiding warranties for a living since 2018
- Projects :
  - Done :
    - Bypassing the Hantek DSO software limitation
    - GPS spoofing on DJI Inspire 1
    - Recovering and exploiting IP cameras
  - WIP :
    - Freeway toll gate token reverse engineering
    - NOVAL 4G IoT xxxxx 😉

Twitter / X : @CyberWolf_2077

Blog : whiterose-infosec.super.site/

ared

1.

Why ?

observation

For students :

- Hardware => Electronic === Math

For me :

- Hardware => practical and fun

We do not need math to do hardware.

Can help nonetheless to avoid forking things up

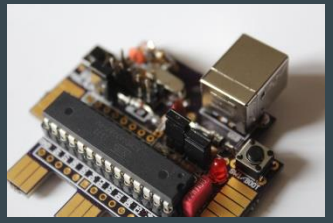
My students wanted to do hardware but :

- Don’t know much about math (neither do I, I am an hyena after all)
- Unfamiliar with comm protocols (SPI, I2C, UART ….)
- Don’t know how to read a PDF (Datasheet ?)
- Don’t know about tools that are needed (Logic analyser, oscillo…what?)

A simple idea at start

Idea :

- A small CTF
- Based on ATMega328p
- Not a lot of equipments needed
- Simple flags for an easy introduction to hardware

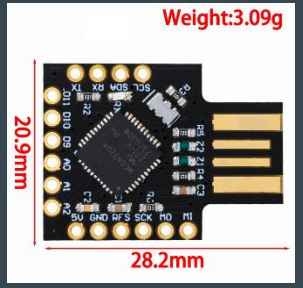


Issue :

- ATMega328p is old
- I don’t have a lot of ‘em

Solution :

- I have lotta ’ATMega32U4 (shitty Ducky)
- 32U4 is the evolution of 328p
- Similaire characteristics
- Several form factors
- inexpensive



Little recap :

mail.google.com

Utilisation de la mémoire :

566 Mo

ared

2.

Result

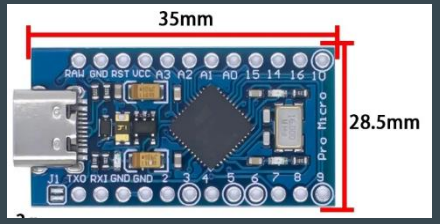
Mini CTF Hardware :

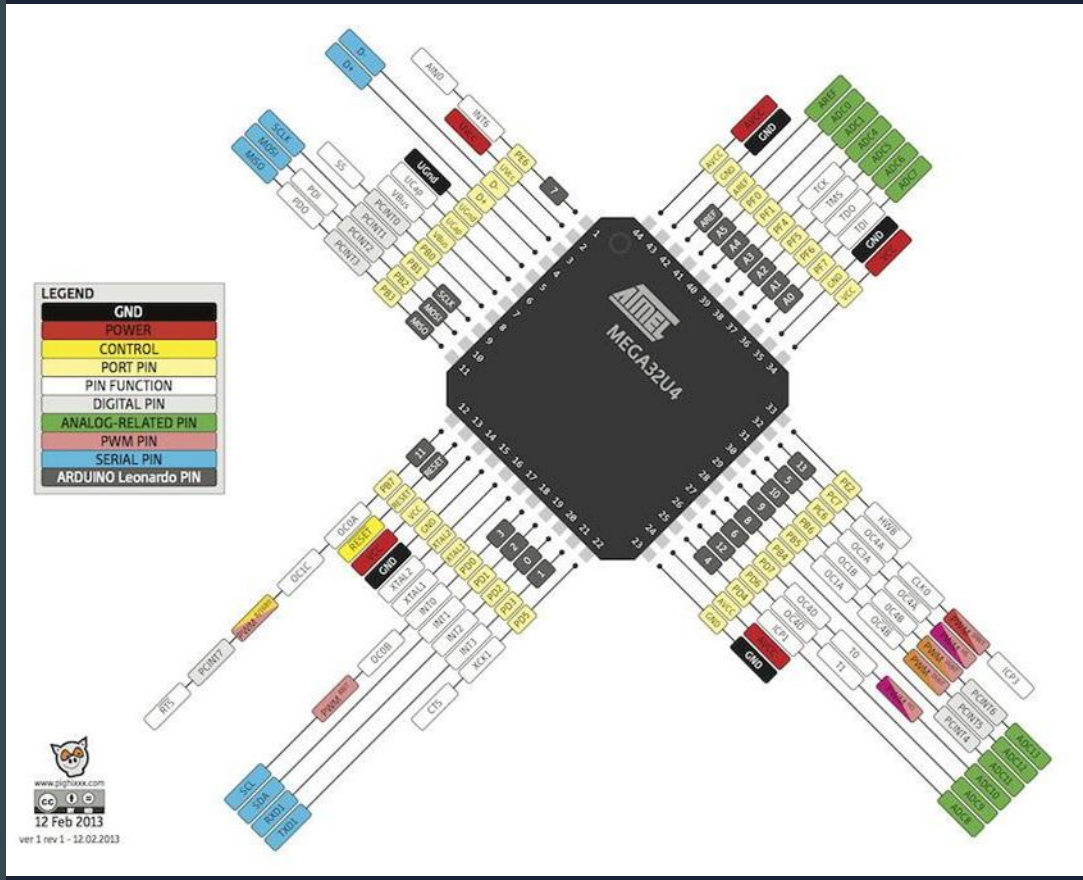
Objectifs :

- Learning how to read docs (CTRL+F on Datasheet)
- Discover protocols (SPI,UART,I2C, …)
- Use tools (Logic Analyser, oscilloscope)
- Practice
- Remember that we can do lotta shit with not a lot

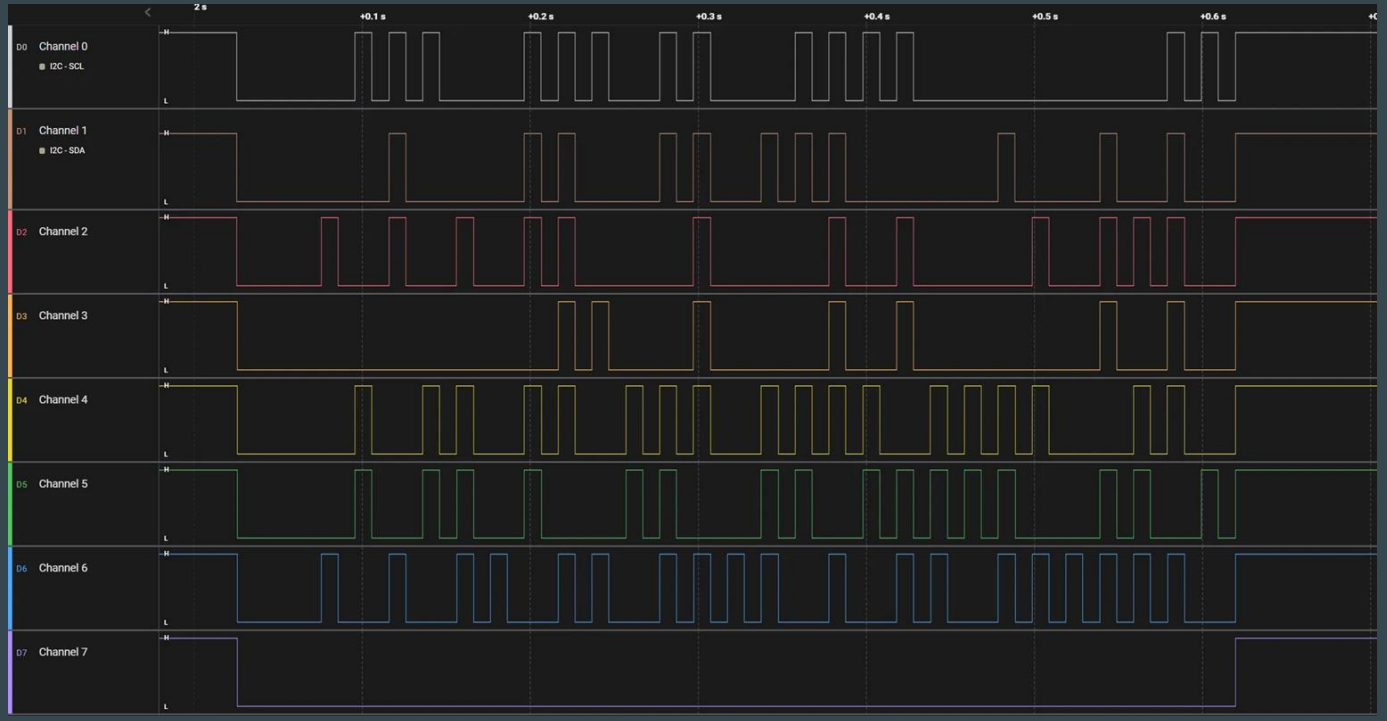
Result :

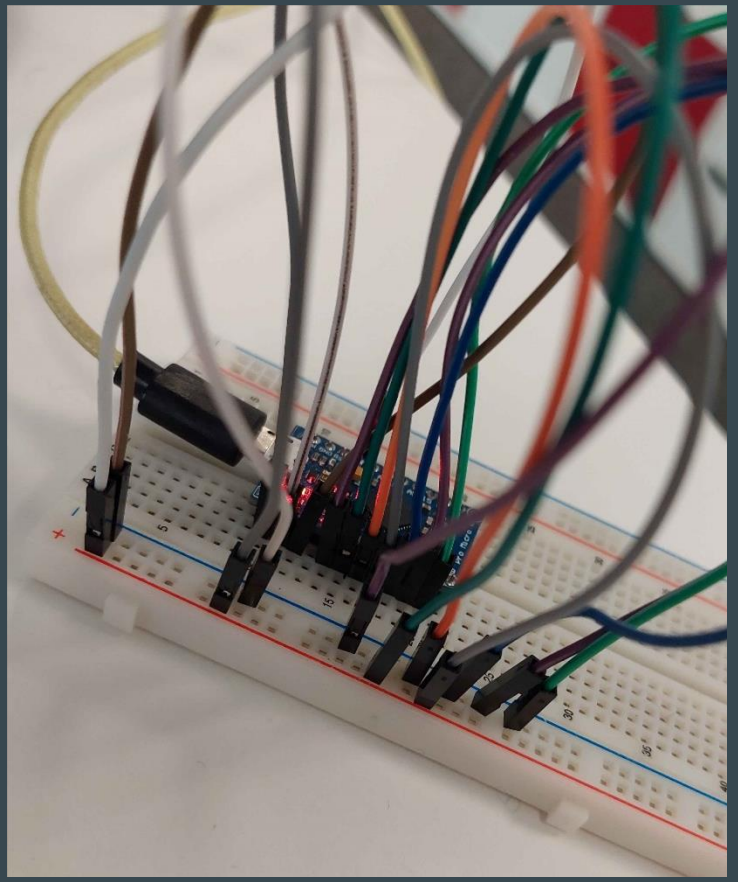
- 14 Flags
- Usage 50% ROM and 90% RAM
- Lotta fun, or not
- Multi platform -> ESP32-WROOM



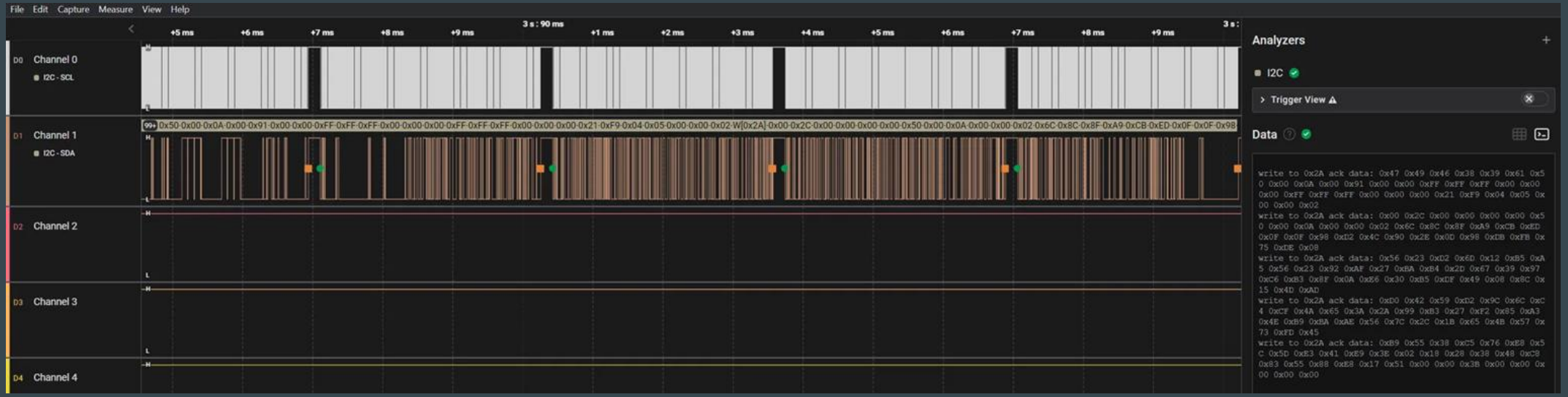


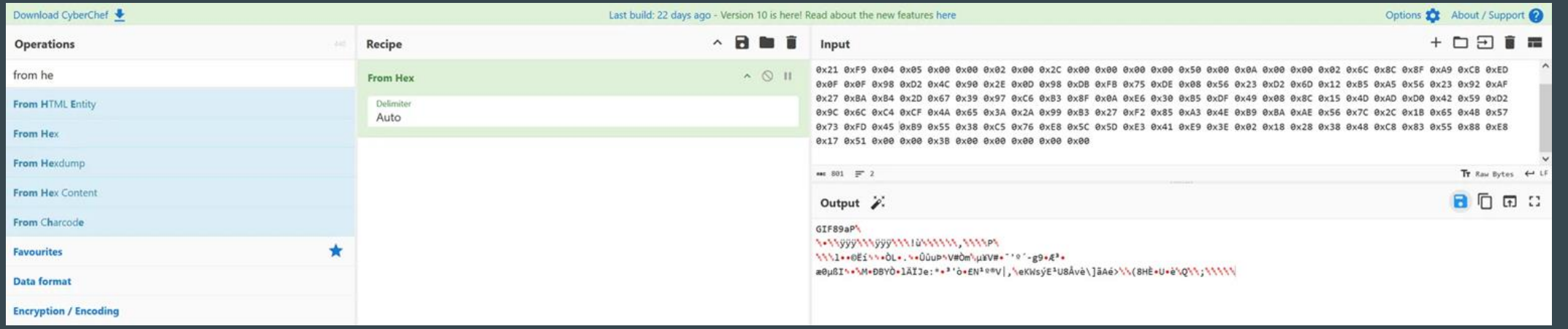
Some pics





Some pics





ared

2.

Future ?

Bullying my students moar

- I2C Screen interception
- DPA (Differential Power Analysis
- Fault Injection
- Code dump